Criptosistemas de Chave Pública Baseados no Problema do Logaritmo Discreto

Prof. Dr. Iaçanã Ianiski Weber

Confiabilidade e Segurança de Software

98G08-4

Agradecimentos especiais ao Prof. Avelino Zorzo e aos Autores Christof Paar e Jan Pelzl pelo material.

Índice

Índice

Troca de Chaves Diffie-Hellman: Visão Geral

- Proposto em 1976 por Whitfield Diffie e Martin Hellman
- Amplamente utilizado, e.g., em Secure Shell (SSH), Transport Layer Security (TLS) e Internet Protocol Security (IPSec)
- O Diffie-Hellman Key Exchange (DHKE) é um protocolo de troca de chaves e **não** utilizado para criptografia

  (Para fins de criptografia baseada no DHKE, o ElGamal pode ser utilizado.)

Troca de Chaves Diffie-Hellman: Configuração Inicial

1. Escolha um primo grande p.
2. Escolha um inteiro $\alpha \in \{2, 3, \ldots, p-2\}$.
3. Publique p e α.

Troca de Chaves Diffie-Hellman: Protocolo

Alice		**Bob**
Escolhe key privada aleatória $k_{prA} = a \in \{1, 2, \ldots, p-1\}$		Escolhe key privada aleatória $k_{prB} = b \in \{1, 2, \ldots, p-1\}$
Calcula key pública correspondente $k_{pubA} = A = \alpha^a \bmod p$	$\xrightarrow{A}$	
	$\xleftarrow{B}$	Calcula key pública correspondente $k_{pubB} = B = \alpha^b \bmod p$
Calcula segredo comum $k_{AB} = B^a = (\alpha^b)^a \bmod p$		Calcula segredo comum $k_{AB} = A^b = (\alpha^a)^b \bmod p$

Podemos agora usar a key conjunta k_{AB} para criptografia, e.g., com AES:

$$y = \text{AES}_{k_{AB}}(x) \xrightarrow{y} x = \text{AES}^{-1}_{k_{AB}}(y)$$

Troca de Chaves Diffie-Hellman: Exemplo

Parâmetros: $p = 29$, $\alpha = 2$

Alice		**Bob**
Escolhe key privada aleatória $k_{prA} = a = 5$		Escolhe key privada aleatória $k_{prB} = b = 12$
Calcula key pública correspondente $k_{pubA} = A = 2^5 = 3 \bmod 29$	$\xrightarrow{3}$	
	$\xleftarrow{7}$	Calcula key pública correspondente $k_{pubB} = B = 2^{12} = 7 \bmod 29$
Calcula segredo comum $k_{AB} = B^a = 7^5 = 16 \bmod 29$		Calcula segredo comum $k_{AB} = A^b = 3^{12} = 16 \bmod 29$

Prova de correção

Alice calcula: $B^a = (\alpha^b)^a \bmod p$

Bob calcula: $A^b = (\alpha^a)^b \bmod p$

Ou seja, Alice e Bob calculam a mesma key k_{AB}!

Índice

O Problema do Logaritmo Discreto

Problema do Logaritmo Discreto (*Discrete Logarithm Problem* - DLP) em $\mathbb{Z}_p^*$.

- Dado o grupo cíclico finito $\mathbb{Z}_p^*$ de ordem $p-1$, um elemento primitivo $\alpha \in \mathbb{Z}_p^*$ e outro elemento $\beta \in \mathbb{Z}_p^*$.
- O DLP é o problema de determinar o inteiro x tal que $1 \leq x \leq p-1$ e $\alpha^x \equiv \beta \bmod p$.
- Esta computação é chamada de **problema do logaritmo discreto**.

$$x = \log_\alpha \beta \bmod p$$

- Exemplo: Calcule x para $5^x \equiv 41 \bmod 47$.

O Problema do Logaritmo Discreto Generalizado

- Dado um grupo cíclico finito G com a operação de grupo $\circ$ e cardinalidade n.
- Consideramos um elemento primitivo $\alpha \in G$ e outro elemento $\beta \in G$.
- O problema do logaritmo discreto consiste em encontrar o inteiro x, onde $1 \leq x \leq n$, tal que:

$$\beta = \underbrace{\alpha \circ \alpha \circ \ldots \circ \alpha}_{x \text{ vezes}} = \alpha^x$$

O Problema do Logaritmo Discreto Generalizado

Os seguintes problemas de logaritmo discreto foram propostos para uso em criptografia:

1. O grupo multiplicativo do corpo primo $\mathbb{Z}_p$ ou um subgrupo dele. Por exemplo, o DHKE clássico utiliza este grupo (slides anteriores), mas também a criptografia Elgamal ou o Digital Signature Algorithm (DSA).
2. O grupo cíclico formado por uma curva elíptica.
3. O grupo multiplicativo de um corpo de Galois $GF(2^m)$ ou um subgrupo dele. Esquemas como o DHKE podem ser realizados com eles.
4. Curvas hiperelípticas ou variedades algébricas, que podem ser vistas como generalizações de curvas elípticas.

Observação: Os grupos 1. e 2. são os mais frequentemente utilizados na prática.

Índice

Ataques contra o Problema do Logaritmo Discreto

- A segurança de muitas primitivas assimétricas baseia-se na dificuldade de calcular o DLP em grupos cíclicos, i.e., calcular x para dados α e β tais que:

$$\beta = \underbrace{\alpha \circ \alpha \circ \ldots \circ \alpha}_{x \text{ vezes}} = \alpha^x$$

- Existem os seguintes algoritmos para calcular logaritmos discretos:
  - Algoritmos genéricos: Funcionam em qualquer grupo cíclico
    - Busca por Força Bruta
    - Método Baby-Step-Giant-Step de Shanks
    - Método Rho de Pollard
    - Método de Pohlig-Hellman
  - Algoritmos não genéricos: Funcionam apenas em grupos específicos, em particular em $\mathbb{Z}_p$
    - Método do Cálculo de Índices
- **Observação:** Curvas elípticas só podem ser atacadas com algoritmos genéricos, que são mais fracos que os algoritmos não genéricos. Portanto, curvas elípticas são seguras com comprimentos de key menores do que o DLP em corpos primos $\mathbb{Z}_p$.

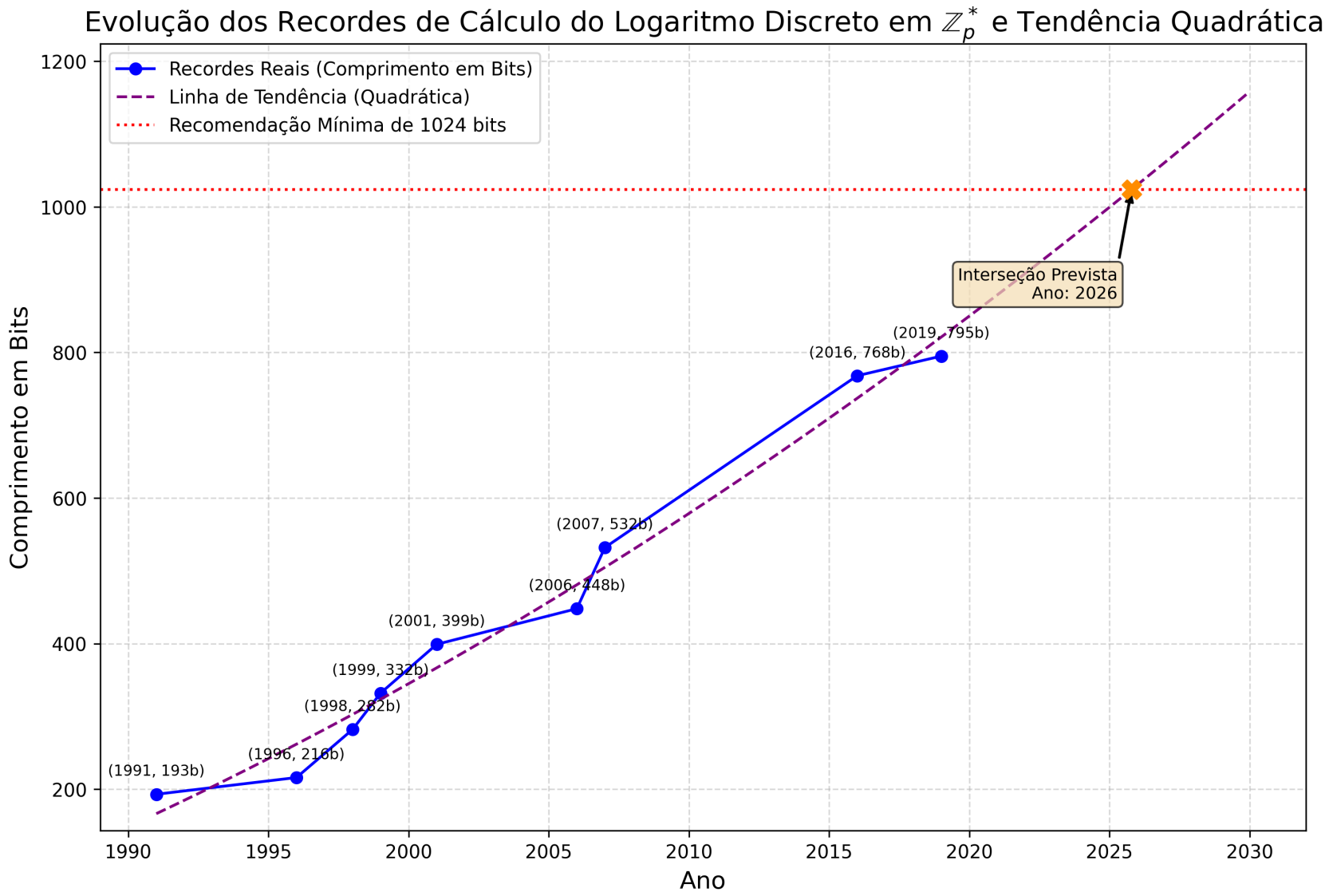
Ataques contra o Problema do Logaritmo Discreto

Resumo dos recordes para o cálculo de logaritmos discretos em $\mathbb{Z}_p^*$:

Dígitos decimais	**Comprimento em bits**	**Data**
58	193	1991
68	216	1996
85	282	1998
100	332	1999
120	399	2001
135	448	2006
160	532	2007
232	768	2016
240	795	2019

A fim de prevenir ataques que calculam o DLP, recomenda-se usar primos com um comprimento de pelo menos 2048 bits para esquemas como o Diffie-Hellman em $\mathbb{Z}_p^*$.

Ataques contra o Problema do Logaritmo Discreto



Segurança da Troca de Chaves Diffie-Hellman Clássica

- Quais informações Oscar possui?
  - α, p
  - $k_{pubA} = A = \alpha^a \bmod p$
  - $k_{pubB} = B = \alpha^b \bmod p$
- Quais informações Oscar quer obter?
  - $k_{AB} = \alpha^{ba} = \alpha^{ab} \bmod p$
  - Isto é conhecido como Problema de Diffie-Hellman (DHP).
- A única forma conhecida de resolver o DHP é resolver o DLP, i.e.,
  1. Calcular $a = \log_\alpha A \bmod p$.
  2. Calcular $k_{AB} = B^a = \alpha^{ba} \bmod p$.

  Conjectura-se que o DHP e o DLP são equivalentes, ou seja, resolver o DHP implica resolver o DLP.
- Para prevenir ataques, ou seja, para prevenir que o DLP possa ser resolvido, escolha $p > 2^{1024}$.

Lições Aprendidas

- O protocolo Diffie-Hellman é um método amplamente utilizado para troca de chaves. Ele é baseado em grupos cíclicos.
- O problema do logaritmo discreto é uma das mais importantes funções de mão única na criptografia assimétrica moderna. Muitos algoritmos de chave pública são baseados nele.
- Para o protocolo Diffie-Hellman em $\mathbb{Z}_p^*$, *o primo p deve ter pelo menos 1024 bits* de comprimento. Isto proporciona uma segurança aproximadamente equivalente a uma cifra simétrica de 80 bits.
- Para uma melhor segurança a longo prazo, um primo de comprimento 2048 bits deve ser escolhido.

Índice

Exercício 1: Cálculo de Chaves DHKE

Calcule as duas chaves públicas e a chave conjunta k_{AB} para o esquema DHKE com os parâmetros $p = 467, \alpha = 2$, e os seguintes pares de chaves privadas (a, b):

- $a = 3, b = 5$
- $a = 400, b = 134$
- $a = 228, b = 57$

Em todos os casos, realize o cálculo da chave conjunta tanto do ponto de vista de Alice quanto de Bob. Isso servirá como uma verificação dos seus resultados.

Exercício 2: Chaves Privadas no DHKE

No protocolo DHKE, as chaves privadas são escolhidas do conjunto

$$\{2, \ldots, p-2\}$$

Por que os valores 1 e $p-1$ são excluídos? Descreva a fraqueza desses dois valores.

Explicação: Fraqueza das Chaves Privadas 1 e $p-1$

A exclusão dos valores 1 e $p-1$ para chaves privadas no protocolo Diffie-Hellman (DHKE) é crucial para a segurança. Vejamos as fraquezas associadas a cada um:

Caso 1: Chave Privada $a = 1$

- **Chave Pública de Alice (A):** Se Alice escolhe $a = 1$, sua chave pública se torna:
$$A = \alpha^a \pmod{p} = \alpha^1 \pmod{p} = \alpha \pmod{p}$$
- **Chave Conjunta (K_{AB}):** A chave conjunta calculada por Alice seria:
$$K_{AB} = B^a \pmod{p} = B^1 \pmod{p} = B \pmod{p}$$
- **Fraqueza:** A chave conjunta é simplesmente a chave pública de Bob (B). Se um invasor (Oscar) interceptar B (que é transmitido publicamente), ele conhecerá diretamente a chave secreta K_{AB}. Alice não adiciona nenhuma entropia ou segurança à chave.

Explicação: Fraqueza das Chaves Privadas 1 e $p-1$

Caso 2: Chave Privada $a = p - 1$

- **Contexto (Pequeno Teorema de Fermat):** Se p é um número primo, então para qualquer inteiro α não divisível por p, temos $\alpha^{p-1} \equiv 1 \pmod{p}$.
- **Chave Pública de Alice (A):** Se Alice escolhe $a = p - 1$, sua chave pública se torna:

$$A = \alpha^a \pmod{p} = \alpha^{p-1} \pmod{p} \equiv 1 \pmod{p}$$

- **Chave Conjunta (K_{AB}):** A chave conjunta calculada por Alice seria:

$$K_{AB} = B^a \pmod{p} = B^{p-1} \pmod{p}$$

Considerando que $B = \alpha^b \pmod{p}$ e $B \not\equiv 0 \pmod{p}$, então $B^{p-1} \equiv 1 \pmod{p}$.

$$K_{AB} \equiv 1 \pmod{p}$$

- **Fraqueza:** A chave conjunta resultante é sempre 1. Uma chave secreta de valor 1 é trivial, previsível e não oferece segurança alguma.